Optimal Unambiguous State Discrimination of two density matrices and its link with the Fidelity

Philippe Raynal and Norbert Lütkenhaus
Quantum Information Theory Group, Institut für Theoretische Physik I, and Max-Plank-Forschungsgruppe, Institut für Optik, Information und Photonik Universität Erlangen-Nürnberg, Staudtstr. 7, D-91058 Erlangen, Germany
(Dated: February 1, 2008)

Recently the problem of Unambiguous State Discrimination (USD) of mixed quantum states has attracted much attention. So far, bounds on the optimum success probability have been derived [1]. For two mixed states they are given in terms of the fidelity. Here we give tighter bounds as well as necessary and sufficient conditions for two mixed states to reach these bounds. Moreover we construct the corresponding optimal measurement strategies. With this result, we provide analytical solutions for unambiguous discrimination of a class of generic mixed states. This goes beyond known results which are all reducible to some pure state case. Additionally, we show that examples exist where the bounds cannot be reached.

I. INTRODUCTION

Quantum state discrimination [2] is a fundamental task in quantum information theory, especially in a communication context. Whenever the signal states are nonorthogonal, perfect discrimination becomes impossible. One has then to resort to optimum state discrimination strategies by specifying figures of merit that define some optimal strategies. The optimum strategy depends then on the quantum states and their *a priori* probabilities. One strategy is *Minimum Error Discrimination* (MED) [2] in which the measurement identifies the possible input states with some error. It is the goal to minimize the error. Another strategy is to optimize the mutual information between the sender and receiver.

The scenario studied here is *Unambiguous State Discrimination* (USD) which characterizes a measurement which either identifies a signal state without error ('unambiguous') or sends out a flag stating that it failed to identify the state. The objective is to minimize this failure probability. The problem of finding optimal USD strategies has been solved for many pure state scenarios [3, 4, 5, 6, 7], including any two pure states [8].

In contrast to the MED problem, which is already solved for any pair of mixed states [2], optimal USD of mixed states is an open problem. Some special cases have been given for which the corresponding problem can be reduced to USD of pure state case, such as in state filtering [9, 10, 11] or state comparison [1, 11]. The underlying reduction theorems have been stated in [12]. For the general case, necessary and sufficient conditions for the optimality of a POVM were derived in [13, 14]. They allow a numerical treatment of the problem but have not given rise to analytic solutions.

For the unambiguous discrimination of a pair of mixed states, lower bounds on the failure probability have been found [1, 15] and reveal three regimes, depending on the ratio between the two *a priori* probabilities of the two mixed states. The boundaries of the middle regime were recently refined in [11] but the consequences for the two remaining outer regimes were not addressed. Here we provide new bounds in those two regimes. Furthermore we derive necessary and sufficient conditions to reach the three bounds in the three different regimes. Given two density matrices ρ_0 and ρ_1 and their *a priori* probabilities η_0 and η_1, the necessary and sufficient conditions to reach the bounds given here take the form of the positivity of two particular operators. Moreover we show that examples exist where the bounds cannot be attained. When the necessary and sufficient conditions are fulfilled, we give the optimal measurement strategy to reach the bounds.

The structure of this paper is the following. In the Sec. II, we derive lower bounds for the success probability in the case of two mixed states. Our derivation uses the Cauchy-Schwarz inequality, as used in [16], and allows us to look for necessary and sufficient conditions to reach the lower bound in each regime of the *a priori* probabilities. In Sec. III, we report the notion of *parallel addition* that leads to some useful relations for USD in connection with a reduction theorem of Ref.[12]. In Sec.IV, we derive the main result of this paper as a theorem: two necessary and sufficient conditions for the failure probability to reach the bounds are given. We also give the corresponding optimal POVM. In Sec.V, we provide examples showing that there are generic mixed states of interest for which the necessary and sufficient conditions are fulfilled and for which we can therefor give the optimal USD measurement.

II. LOWER BOUNDS ON THE FAILURE PROBABILITY

In Unambiguous State Discrimination, the performed measurement either identifies uniquely a state (conclusive result) or fails to identity it (inconclusive result). The goal is to optimize that strategy by finding the measurement for which the probability of inconclusive result is as small as possible. The problem is then specified by the set of quantum signal states $\{\rho_i\}$ and their respective *a priori* probabilities $\{\eta_i\}$. The measurement is a generalized measurement i.e. a Positive Operator-Valued Measure (POVM) [2]. A POVM is a set of hermitian and positive semi-definite operators $\{E_i\}_i$ that add up to identity acting on the Hilbert space spanned by the signal states, i.e. $\sum_i E_i = \mathbb{1}_{\mathcal{H}}$. Given N possible input states, we consider measurements with $N+1$ outcomes where the first N outcomes identify a state and the last one corresponds to inconclusive results where the identification failed. The POVM elements are denoted by E_k with $k = 1, \ldots, N$ and $E_?$ respectively. The probability to obtain an outcome for some POVM element E for a given signal ρ is then given by $\mathrm{Tr}(E\rho)$.

In general, a POVM describing a USD measurement satisfies $\mathrm{Tr}(E_k\rho_i) = 0$ whenever $k \neq i$ so that only the state ρ_i can trigger the measurement outcome connected to E_k. The failure probability Q of a USD strategy is then given by $Q = \sum_i Q_i$, where $Q_i = \sum_i \eta_i \mathrm{Tr}(E_?\rho_i)$. From this definition we find that $Q_i \leq \eta_i$. In this paper, we consider the USD of two signal states ρ_0 and ρ_1 that are mixed states with *a priori* probabilities η_0 and η_1. Accordingly, our POVM contains three elements $\{E_0, E_1, E_?\}$ which correspond respectively to the conclusive detection of ρ_0, to the conclusive detection of ρ_1 and to an inconclusive result. The failure probability then equals $Q = Q_0 + Q_1$.

Our interest is first focused on the product Q_0Q_1. We can give a lower bound that is expressed in terms of the fidelity F of the two states. The fidelity is defined as $F = \mathrm{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$ [17]. The bounds, formulated in the following theorem, are tighter than the one given in [1]. Moreover, we pay additionally attention to the condition under which the bound can be reached.

As for the notation, consider an hermitian and positive semi-definite operators O. We can define its unique square root $\sqrt{O}$ and decompose it into the form $O = MM^\dagger$ with $M = \sqrt{O}U$, for any unitary matrix U. Since the states ρ_i and the POVM elements E_k all are hermitian and positive semi-definite operators, we can introduce their square root and use the previous decomposition.

Theorem 1 *Let ρ_0 and ρ_1 be two density matrices with a priori probabilities η_0 and η_1. We define the fidelity of the two states ρ_0 and ρ_1 as $F = Tr(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$. Then, for any USD measurement, the product of the two probabilities Q_0 and Q_1 to fail to identify respectively the state ρ_0 and ρ_1 is such that*

$$Q_0Q_1 \geq \eta_0\eta_1F^2. \tag{1}$$

The equality holds if and only if the unitary operator V arising from a polar decomposition

$$\sqrt{\rho_0}\sqrt{\rho_1} = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}\, V$$

satisfies

$$V^\dagger\sqrt{\rho_0}E_? = \alpha\sqrt{\rho_1}E_? \tag{2}$$

for some $\alpha \in \mathbb{R}^+$.

Before we turn to the proof of this theorem note that relation (2) implies a condition required for the optimality of a USD POVM (see [10, 12]). It is clear that optimality of a specific USD measurement implies that the conditional states after the inconclusive results do not allow further USD measurements. That would already be satisfied if, for example, the supports of the conditional states coincide. We find a stronger property whenever equality holds in Theorem 1. Indeed, if we have $V^\dagger\sqrt{\rho_0}E_? = \alpha\sqrt{\rho_1}E_?$ with $\alpha \in \mathbb{R}^+$, then it follows immediately that $\sqrt{E_?}\rho_0\sqrt{E_?} = \alpha^2\sqrt{E_?}\rho_1\sqrt{E_?}$. This means that the conditional states corresponding to inconclusive results must be identical up to normalization. Therefor no information whatsoever about the signal state can be extracted from these conditional states.

Proof of Theorem 1 The basic ingredient for the derivation of the bound is the Cauchy-Schwarz inequality:

Theorem 2 *[18] Cauchy-Schwarz inequality*
If x and y are members of a unitary space then $\|x\|\|y\| \geq |(x, y)|$. The equality holds if and only if $x = \alpha\, y$ for some α in $\mathbb{C}$.

A unitary space is a complex linear space $\mathcal{S}$ together with an inner product from $\mathcal{S} \times \mathcal{S}$ to $\mathbb{C}$. Therefore the complex space of bounded operators acting on a Hilbert space is a complete unitary space if we consider for two elements A, B

the inner product $\mathrm{Tr}(AB^\dagger)$. Hence, with $E_i = M_i M_i^\dagger$, $\rho_0 = \sqrt{\rho_0} U U^\dagger \sqrt{\rho_0}$ and $\rho_1 = \sqrt{\rho_1}\sqrt{\rho_1}$, we obtain

$$\begin{aligned}\sqrt{\mathrm{Tr}(E_i\rho_0)}\sqrt{\mathrm{Tr}(E_i\rho_1)} &= \sqrt{\mathrm{Tr}(U\sqrt{\rho_0}M_iM_i^\dagger\sqrt{\rho_0}U^\dagger)}\sqrt{\mathrm{Tr}(\sqrt{\rho_1}M_iM_i^\dagger\sqrt{\rho_1})}\\ &\geq |\mathrm{Tr}(U\sqrt{\rho_0}M_iM_i^\dagger\sqrt{\rho_1})|,\end{aligned}$$

where we have used the freedom in the decomposition of ρ_0. By Theorem 2, the equality holds if and only if $U\sqrt{\rho_0}M_i = \alpha\sqrt{\rho_1}M_i$, for some $\alpha \in \mathbb{C}$ or, equivalently, if and only if $U\sqrt{\rho_0}E_i = \alpha\sqrt{\rho_1}E_i$, for some $\alpha \in \mathbb{C}$.
We now consider a USD POVM $\{E_i\}_{i=0,1,?}$. Using the fact that $\mathrm{Tr}(E_0\rho_1) = \mathrm{Tr}(E_1\rho_0) = 0$, we find for E_0 and E_1

$$\begin{aligned}0 = \sqrt{\mathrm{Tr}(E_0\rho_0)}\sqrt{\mathrm{Tr}(E_0\rho_1)} \geq |\mathrm{Tr}(U\sqrt{\rho_0}E_0\sqrt{\rho_1})|,\\ 0 = \sqrt{\mathrm{Tr}(E_1\rho_0)}\sqrt{\mathrm{Tr}(E_1\rho_1)} \geq |\mathrm{Tr}(U\sqrt{\rho_0}E_1\sqrt{\rho_1})|.\end{aligned}$$

This simply means that $\mathrm{Tr}(U\sqrt{\rho_0}E_0\sqrt{\rho_1}) = \mathrm{Tr}(U\sqrt{\rho_0}E_1\sqrt{\rho_1}) = 0$. For $E_?$, we obtain

$$\sqrt{\mathrm{Tr}(E_?\rho_0)}\sqrt{\mathrm{Tr}(E_?\rho_1)} \geq |\mathrm{Tr}(U\sqrt{\rho_0}E_?\sqrt{\rho_1})|.$$

From this it follows that we can write

$$\sqrt{\mathrm{Tr}(E_?\rho_0)}\sqrt{\mathrm{Tr}(E_?\rho_1)} \geq |\mathrm{Tr}(U\sqrt{\rho_0}E_?\sqrt{\rho_1}) + 0 + 0| = |\mathrm{Tr}(U\sqrt{\rho_0}\sqrt{\rho_1})|\,, \tag{3}$$

where we used the relation $\sum_i E_i = \mathbb{1}$. Furthermore, the inequality (3) must hold for any unitary matrix U so that we find

$$\sqrt{\mathrm{Tr}(E_?\rho_0)}\sqrt{\mathrm{Tr}(E_?\rho_1)} \geq \max_U |\mathrm{Tr}(U\sqrt{\rho_0}\sqrt{\rho_1})|. \tag{4}$$

Here, again, the equality holds if and only if a unitary operator $U_{\max}$ which maximizes the right hand side satisfies

$$U_{\max}\sqrt{\rho_0}E_? = \alpha\sqrt{\rho_1}E_?$$

for some $\alpha \in \mathbb{C}$. To find the unitary matrices $U_{\max}$ that maximize $|\mathrm{Tr}(U\sqrt{\rho_0}\sqrt{\rho_1})|$ we use the following lemma:

Lemma 1 *For any operator A in the space M_n of $n \times n$ matrices we find*

$$\max_U |\,Tr(AU)| = Tr(|A|)$$

where the maximum is taken over all the unitary matrices. The maximum is reached for any unitary operator U that can be written as $U = V^\dagger e^{\imath\phi}$. Here $e^{\imath\phi}$ is an arbitrary phase while the unitary operator V is defined via the polar decomposition

$$A = |A|\,V$$

with $|A| = \sqrt{AA^\dagger} = V\sqrt{A^\dagger A}\,V^\dagger$.

Proof For any operator A, we can introduce its polar decomposition $A = |A|\,V$ with $|A| = \sqrt{AA^\dagger} = V\sqrt{A^\dagger A}\,V^\dagger$. Note that V is unitary while $\sqrt{AA^\dagger}$ and $\sqrt{A^\dagger A}$ are unique, positive semi-definite and hermitian. With that we find

$$|\mathrm{Tr}(AU)| = |\mathrm{Tr}(|A|VU)| = |\mathrm{Tr}(|A|^{1/2}|A|^{1/2}VU)|.$$

We denote $X = |A|^{1/2} = X^\dagger$ and $Y = |A|^{1/2}VU$ and apply the Cauchy-Schwarz inequality (Theorem 2) to obtain

$$|\mathrm{Tr}(AU)| = |\mathrm{Tr}(X^\dagger Y)| \leq \sqrt{\mathrm{Tr}(|A|)}\,\sqrt{\mathrm{Tr}(U^\dagger V^\dagger |A| VU))} = \mathrm{Tr}(|A|)\,.$$

Equality holds if and only if $|A|^{1/2} = \beta|A|^{1/2}VU$, for some $\beta \in \mathbb{C}$. This is possible if and only if $\beta VU = \mathbb{1}$, where U and V are both unitary matrices. This means that $\beta = e^{-\imath\phi}$ for some ϕ so that we find the connection $U = V^\dagger e^{\imath\phi}$. This completes the proof of the lemma.

Thanks to lemma 1, Eqn. (4) implies

$$\sqrt{\mathrm{Tr}(E_?\rho_0)}\sqrt{\mathrm{Tr}(E_?\rho_1)} \geq |\mathrm{Tr}(|\sqrt{\rho_0}\sqrt{\rho_1}|)|$$

where equality now holds if and only if

$$V^\dagger e^{\imath\phi}\sqrt{\rho_0}E_?=\alpha\sqrt{\rho_1}E_? \tag{5}$$

for some $\alpha\in\mathbb{C}$. Let us introduce the operators $F_0:=|\sqrt{\rho_0}\sqrt{\rho_1}|=\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $F_1=V^\dagger F_0 V=\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$, which are motivated by the polar decomposition

$$\sqrt{\rho_0}\sqrt{\rho_1}=F_0V=VF_1. \tag{6}$$

These operators are related to the fidelity of the two density matrices through the relation $F=\mathrm{Tr}(\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}})(=\mathrm{Tr}(F_0)=\mathrm{Tr}(F_1))$ ([17]).

Next we use the definitions of the partial failure probabilities $Q_i=\eta_i\mathrm{Tr}(E_?\rho_i)$ and choose the phase $e^{\imath\phi}$ to be the same as the phase of α in (5) to obtain the desired inequality $Q_0Q_1\geq\eta_0\eta_1F^2$. Equality in the previous equation then holds if and only if $V^\dagger\sqrt{\rho_0}E_?=\alpha\sqrt{\rho_1}E_?$, for some $\alpha\in\mathbb{R}^+$. This completes the proof. ■

We can now derive the bounds in the different regimes of the ratio $\frac{\eta_1}{\eta_0}$ between the two *a priori* probabilities. Actually, the procedure is to find the minimum of the failure probability $Q=Q_0+Q_1$ under the constraints of the previous derived inequality $Q_0Q_1\geq\eta_0\eta_1F^2$. According to Theorem 1, we can provide the necessary and sufficient condition for equality.

Theorem 3 *Let ρ_0 and ρ_1 be two density matrices with a priori probabilities η_0 and η_1. We define the fidelity F of the two states ρ_0 and ρ_1 as $Tr(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$. We denote by P_0 and P_1, the projectors onto the support of ρ_0 and ρ_1. Then, for any USD measurement, the failure probability Q obeys*

$$\begin{aligned}
Q&\geq\eta_1\frac{F^2}{Tr(P_1\rho_0)}+\eta_0\,Tr(P_1\rho_0)\quad for\quad \sqrt{\frac{\eta_1}{\eta_0}}\leq\frac{Tr(P_1\rho_0)}{F}\\
Q&\geq 2\sqrt{\eta_0\eta_1}F\quad for\quad \frac{Tr(P_1\rho_0)}{F}\leq\sqrt{\frac{\eta_1}{\eta_0}}\leq\frac{F}{Tr(P_0\rho_1)}\\
Q&\geq\eta_0\frac{F^2}{Tr(P_0\rho_1)}+\eta_1\,Tr(P_0\rho_1)\quad for\quad \frac{F}{Tr(P_0\rho_1)}\leq\sqrt{\frac{\eta_1}{\eta_0}}\,.
\end{aligned} \tag{7}$$

Equality holds if and only if the unitary operator V arising from a polar decomposition $\sqrt{\rho_0}\sqrt{\rho_1}=\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}\,V$ satisfies $V^\dagger\sqrt{\rho_0}E_?=\alpha\sqrt{\rho_1}E_?$, with $\alpha=\frac{Tr(P_1\rho_0)}{F}$, $\alpha=\sqrt{\frac{\eta_1}{\eta_0}}$ and $\alpha=\frac{F}{Tr(P_0\rho_1)}$ in the the first, second and third regime, respectively.

Proof First of all, according to Theorem 1, we know that for any USD measurement the inequality $Q_1\geq\frac{\eta_0\eta_1F^2}{Q_0}$ holds. It follows that the failure probability is such that

$$Q\geq Q_0+\frac{\eta_0\eta_1F^2}{Q_0}\,. \tag{8}$$

Let us consider relations that only hold if equality holds in Eqn. (8). In this case we have

$$Q_0Q_1=\eta_0\eta_1F^2\,. \tag{9}$$

Moreover, from Theorem 1 we know that in this case we have $V^\dagger\sqrt{\rho_0}E_?=\alpha\sqrt{\rho_1}E_?$, for some $\alpha\in\mathbb{R}^+$. This relationship implies, via the respective definitions, that

$$Q_0=\alpha^2\frac{\eta_0}{\eta_1}Q_1\,. \tag{10}$$

We can combine the two equations (9) and (10) to

$$Q_0=\alpha\eta_0F\,. \tag{11}$$

So the final statement is that $Q=Q_0+\frac{\eta_0\eta_1F^2}{Q_0}$ if and only if $V^\dagger\sqrt{\rho_0}E_?=\alpha\sqrt{\rho_1}E_?$, where α now is explicitly related to the other parameters as $Q_0=\alpha\eta_0F$.

Second, we have to derive the range constraint on Q_0 and Q_1. We know already that $Q_i\leq\eta_i$. Moreover, from the work by Herzog and Bergou in [11], we learn that $\eta_0\mathrm{Tr}(P_1\rho_0)\leq Q_0$ and $\eta_1\mathrm{Tr}(P_0\rho_1)\leq Q_1$. Indeed, from the structure of the POVM elements, we have $E_0+E_1+E_?=\mathbb{1}$ with $\mathcal{S}_{E_0}\subset\mathcal{S}_{\rho_1}^\perp$ and $\mathcal{S}_{E_1}\subset\mathcal{S}_{\rho_0}^\perp$. We consider only the non-trivial

case where the supports of ρ_0 and ρ_1 are not identical. Then its structure must be such that $E_1+E_? = P_1+R$ where P_1 is the projection onto the support of ρ_1 and R is an hermitian positive semi-definite operator with support $\mathcal{S}_R \subset \mathcal{S}_{\rho_1}^{\perp}$ which satisfies $E_0 + R = P_1^{\perp}$. Then it follows that $P_0 = \eta_0 \mathrm{Tr}(E_0\rho_0) = \eta_0 \mathrm{Tr}(P_1^{\perp}\rho_0) - \eta_0 \mathrm{Tr}(R\rho_0)$. In our non-trivial case we will have $\mathrm{Tr}(R\rho_0) > 0$ as soon as $R \neq 0$. This yields $P_0 \leq \eta_0 \mathrm{Tr}(P_1^{\perp}\rho_0)$ or equivalently $Q_0 \geq \eta_0 \mathrm{Tr}(P_1\rho_0)$. In the same way, on can find $Q_1 \geq \eta_1 \mathrm{Tr}(P_0\rho_1)$. We then have

$$\begin{aligned} \eta_0 \mathrm{Tr}(P_1\rho_0) \leq Q_0 \leq \eta_0, \\ \eta_1 \mathrm{Tr}(P_0\rho_1) \leq Q_1 \leq \eta_1. \end{aligned} \tag{12}$$

These two constraints can be combined to $\eta_0 \mathrm{Tr}(P_1\rho_0) \leq Q_0 \leq \eta_0 \frac{F^2}{\mathrm{Tr}(P_0\rho_1)}$. This can be seen as follows. Since $Q_1 = \frac{\eta_0\eta_1 F^2}{Q_0}$, the constraints on Q_1 take the form $\eta_0 F^2 \leq Q_0 \leq \eta_0 \frac{F^2}{\mathrm{Tr}(P_0\rho_1)}$. Let us consider the USD POVM given by $\{E_? = P_1, E_0 = P_1^{\perp}, E_1 = 0\}$. Thank to Theorem 1, we find $\eta_0\eta_1 F^2 \leq \eta_0\eta_1 \mathrm{Tr}(P_1\rho_0)\mathrm{Tr}(P_1\rho_1)$ or in other words $\eta_0 F^2 \leq \eta_0 \mathrm{Tr}(P_1\rho_0)$. We can also consider the USD POVM given by $\{E_? = P_0, E_0 = 0, E_1 = P_0^{\perp}\}$ and with Theorem 1, we finally have $\eta_0 \frac{F^2}{\mathrm{Tr}(P_0\rho_1)} \leq \eta_0$.

Next, we define the function $q(Q_0) = Q_0 + \frac{\eta_0\eta_1 F^2}{Q_0}$ and minimize it under the constraint $\eta_0 \mathrm{Tr}(P_1\rho_0) \leq Q_0 \leq \eta_0 \frac{F^2}{\mathrm{Tr}(P_0\rho_1)}$. The resulting minimum will constitute a lower bound for Q. The function $q(Q_0)$ is convex ($\frac{d^2q}{dQ_0^2}(Q_0) \geq 0$) and, therefore, it takes its minimum at the point $Q_0^{\min}$ where the derivative vanishes ($\frac{dq}{dQ_0}(Q_0) = 0$ yielding $Q_0^{\min} = \sqrt{\eta_0\eta_1}F$) or at the limits of the constraint interval ($Q_0^{\min} = \eta_0 \mathrm{Tr}(P_1\rho_0)$ and $Q_0^{\min} = \eta_0 \frac{F^2}{\mathrm{Tr}(P_0\rho_1)}$). That gives us the minimum in three different regimes. In the first regime we have $q_{\min}(Q_0) = \eta_0 \mathrm{Tr}(P_1\rho_0) + \eta_1 \frac{F^2}{\mathrm{Tr}(P_1\rho_0)}$ and $Q_0^{\min} = \eta_0 \mathrm{Tr}(P_1\rho_0)$ if $\sqrt{\eta_0\eta_1}F \leq \eta_0 \mathrm{Tr}(P_1\rho_0)$ that is to say if $\sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{\mathrm{Tr}(P_1\rho_0)}{F}$. In the second regime we have $q_{\min}(Q_0) = 2\sqrt{\eta_0\eta_1}F$ and $Q_0^{\min} = \sqrt{\eta_0\eta_1}F$ if $\frac{\mathrm{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\mathrm{Tr}(P_0\rho_1)}$. The third regime gives $q_{\min}(Q_0) = \eta_0 \frac{F^2}{\mathrm{Tr}(P_0\rho_1)} + \eta_1 \mathrm{Tr}(P_0\rho_1)$ and $Q_0^{\min} = \eta_0 \frac{F^2}{\mathrm{Tr}(P_0\rho_1)}$ if $\frac{F}{\mathrm{Tr}(P_0\rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}}$.

As a result we obtain lower bounds for the failure probability Q in three regimes as given in Eqn. (7). For each regime, the value of Q_0 which minimized $q(Q_0)$ is given and via Eqn. (11) we find the corresponding value that α has to take. We read off the values as $\alpha = \frac{\mathrm{Tr}(P_1\rho_0)}{F}$, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ and $\alpha = \frac{F}{\mathrm{Tr}(P_0\rho_1)}$ for the first, second and third regime, respectively. ■

Let us note that, by construction, those bounds are tighter than the ones in [1]. Indeed, one could recover the three bounds in [1] by looking for the minimum of the function $q(Q_0)$ under the weaker constraints $\eta_0 F^2 \leq Q_0 \leq \eta_0$.

III. THE PARALLEL ADDITION $\rho_0 : \rho_1$

Before deriving our central theorem, we will first recall some useful results of linear algebra. We denote by M^{-1} the pseudo-inverse of a matrix M, which has not necessarily full rank. The pseudo-inverse can be defined via the singular-value decomposition of M. Whenever M is of full rank, the pseudo-inverse coincides with the inverse. In general, it is not known how to express the pseudo inverse of a sum $(A+B)^{-1}$ in terms of the pseudo inverses A^{-1} and B^{-1} [19]. However, a related new operation $A(A+B)^{-1}B$, called parallel addition and denoted by $A:B$ has been defined in 1969 by Anderson and Duffin and will turn out useful in our context.

First of all, we denote by $\mathcal{S}_M$, the support of a hermitian and positive semi-definite matrix M. We then have the following property for the parallel addition:

Property 1 [20] *Let A and B be two hermitian and positive semi-definite matrices in M_n, then the support $\mathcal{S}_{A:B}$ of $A:B$ is given in terms of the supports of A and B as*

$$\mathcal{S}_{A:B} = \mathcal{S}_A \cap \mathcal{S}_B.$$

Next let us recall two reduction theorem for USD of mixed states [12]. We consider the problem of discriminating unambiguously two density matrices ρ_0 and ρ_1 with *a priori* probabilities η_0 and η_1. We denote by r_0 the rank of ρ_0 and by r_1 the rank of ρ_1. A general USD problem can satisfy $r_0 + r_1 \geq d$, where d is the dimension of the Hilbert space $\mathcal{H}$ spanned by the two states. This means in particular that the two supports can overlap.

In a first reduction theorem it has been shown by the authors [12] that any such USD problem can always be reduced to the one of discriminating ρ_0' and ρ_1', two density matrices of rank r_0' and r_1' with *a priori* probabilities η_0'

and η_1', spanning the same Hilbert space $\mathcal{H}$ of dimension $r_0' + r_1'$. Indeed we can split off any common subspace of the supports $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1}$ to end up with $\mathcal{S}_{\rho_0'} \cap \mathcal{S}_{\rho_1'} = \{0\}$. An easy way to know whether the two supports overlap is to check whether the equality $rk(\rho_0') + rk(\rho_1') = rk(\rho_0' + \rho_1')$ holds (see details in [21]). In the reduced case, property (1) implies $\mathcal{S}_{\rho_0' : \rho_1'} = 0$ that is to say $\rho_0' : \rho_1' = 0$. By defining $\Sigma := \rho_0' + \rho_1'$, we can write the parallel addition as $\rho_0' \Sigma^{-1} \rho_1'$. Moreover, since $rk(\rho_0' + \rho_1') = \dim(\mathcal{H})$, we end up with Σ having full-rank and $\Sigma\Sigma^{-1} = \mathbb{1}_{\mathcal{H}}$.

We therefore have the following corollary to property (1),

Corollary 1 *Let ρ_0 and ρ_1 be two density matrices spanning a Hilbert space $\mathcal{H}$. Let Σ be defined as the sum of these two density matrices.*

$$\text{If } \; rk(\rho_0) + rk(\rho_1) = rk(\rho_0 + \rho_1) \; \text{ then } \; \rho_0 \Sigma^{-1} \rho_1 = 0.$$

According to the first reduction theorem we can, without loss of generality, consider only USD problems of two density matrices without overlap of their supports. In the following, we consider two density matrices ρ_0 and ρ_1 (which are hermitian and positive semi-definite matrices) such that $rk(\rho_0 + \rho_1) = rk(\rho_0) + rk(\rho_1) = \dim(\mathcal{H})$. As explained above, for such a problem, $\rho_0 \Sigma^{-1} \rho_1 = 0$, with $\Sigma = \rho_0 + \rho_1$ having full rank. This leads to $\rho_0 \Sigma^{-1} \rho_0 = \rho_0$ and $\rho_1 \Sigma^{-1} \rho_1 = \rho_1$ since $\Sigma\Sigma^{-1} = \mathbb{1}_{\mathcal{H}}$. The projectors onto the supports of those two density matrices can then be written as : $P_{\rho_0} = \sqrt{\rho_0} \Sigma^{-1} \sqrt{\rho_0}$ and $P_{\rho_1} = \sqrt{\rho_1} \Sigma^{-1} \sqrt{\rho_1}$.

A second reduction theorem [12] allows to eliminate the part of the support of ρ_0' which is orthogonal to the support of ρ_1' and *vice et versa*. This implies that the two resulting density matrices ρ_0'' and ρ_1'' possess the same rank r and span a $2r$-dimensional Hilbert space. We denote such a USD problem by "$r + r = 2r$" (see [12] for more details). This second reduction theorem indicates in which situations a further reduction of the original problem can be achieved. This theorem is not needed for the derivation of our central theorem.

IV. NECESSARY AND SUFFICIENT CONDITIONS

We are now ready to derive the main result of this paper. The first part of this result gives compact necessary and sufficient conditions for a pair of mixed states to saturate the bounds of the failure probability Q. The second part gives the corresponding POVMs in an explicit form. To clarify the notation, let us note that in $M \geq 0$ we mean that the operator M is hermitian and positive semi-definite.

Theorem 4 *Necessary and sufficient conditions to saturate the bounds on the failure probability*
Consider a USD problem defined by the two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to [12]). Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $Tr(F_0) = Tr(F_1)$. We denote by P_0 and P_1, the projectors onto the support of ρ_0 and ρ_1. The optimal failure probability Q^{opt} for USD then satisfies

$$Q^{\text{opt}} = \eta_1 \frac{F^2}{Tr(P_1\rho_0)} + \eta_0 \, Tr(P_1\rho_0) \;\; \Leftrightarrow \;\; \begin{array}{l} \rho_0 - \frac{Tr(P_1\rho_0)}{F} F_0 \geq 0 \\ \rho_1 - \frac{Tr(P_1\rho_0)}{F} F_1 \geq 0 \end{array} \;\; \text{for} \;\; \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{Tr(P_1\rho_0)}{F} \tag{13}$$

$$Q^{\text{opt}} = 2\sqrt{\eta_0\eta_1} F \;\; \Leftrightarrow \;\; \begin{array}{l} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0 \end{array} \;\; \text{for} \;\; \frac{Tr(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{Tr(P_0\rho_1)} \tag{14}$$

$$Q^{\text{opt}} = \eta_0 \frac{F^2}{Tr(P_0\rho_1)} + \eta_1 \, Tr(P_0\rho_1) \;\; \Leftrightarrow \;\; \begin{array}{l} \rho_0 - \frac{F}{Tr(P_0\rho_1)} F_0 \geq 0 \\ \rho_1 - \frac{Tr(P_0\rho_1)}{F} F_1 \geq 0 \end{array} \;\; \text{for} \;\; \frac{F}{Tr(P_0\rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}}$$

The POVM elements that realize these optimal failure probabilities, if the corresponding conditions are fulfilled, are given by

$$\begin{aligned} E_0 &= \Sigma^{-1} \sqrt{\rho_0} \, (\rho_0 - \alpha F_0) \sqrt{\rho_0} \Sigma^{-1} \\ E_1 &= \Sigma^{-1} \sqrt{\rho_1} \left(\rho_1 - \frac{1}{\alpha} F_1 \right) \sqrt{\rho_1} \Sigma^{-1} \\ E_? &= \Sigma^{-1} \left(\sqrt{\alpha}\sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} \sqrt{\rho_1} V^\dagger \right) F_0 \left(\sqrt{\alpha}\sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} V \sqrt{\rho_1} \right) \Sigma^{-1} \end{aligned} \tag{15}$$

with $\alpha = \frac{Tr(P_1\rho_0)}{F}$ for the first regime, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ for the second regime and $\alpha = \frac{F}{Tr(P_0\rho_1)}$ for the third regime.

Proof First, we give a proof for the necessary conditions.

Proof for the necessary conditions From Theorem 3 we know that the bounds on the failure probability are satisfied whenever $V^\dagger\sqrt{\rho_0}E_?=\alpha\sqrt{\rho_1}E_?$ with $\alpha=\frac{\mathrm{Tr}(P_1\rho_0)}{F}$, $\alpha=\sqrt{\frac{\eta_1}{\eta_0}}$ and $\alpha=\frac{F}{\mathrm{Tr}(P_0\rho_1)}$ for the three regimes.

We replace $E_?$ by $\mathbb{1}-E_0-E_1$, multiply on the left by V and on the right by $\sqrt{\rho_0}$. This leads us to

$$\rho_0-\alpha F_0=\sqrt{\rho_0}E_0\sqrt{\rho_0} \tag{16}$$

where we used the relation (6) $\sqrt{\rho_0}\sqrt{\rho_1}=F_0V$ and the fact that the support of ρ_i and E_j are orthogonal for $i\neq j$. Indeed, let us notice that $\mathrm{Tr}(E_i\rho_j)=0\Leftrightarrow E_i\rho_j=0$ because E_i and ρ_j are hermitian and positive semi-definite operators [12]. The right hand side in (16) is hermitian and positive semi-definite because of the form $AA^\dagger$ with $A=\sqrt{\rho_0}\sqrt{E_0}$. Then $\rho_0-\alpha F_0$ must be hermitian and positive semi-definite as well. A similar calculation where we only multiply on the right by $\sqrt{\rho_1}$ instead of by $\sqrt{\rho_0}$ leads us to

$$\rho_1-\frac{1}{\alpha}F_1=\sqrt{\rho_1}E_1\sqrt{\rho_1}$$

which is again a hermitian and positive semi-definite operator.

With that we have proved that if equality holds in the bounds of Theorem 3 then we have

$$\begin{aligned}\rho_0-\alpha F_0 &\geq 0\\ \rho_1-\frac{1}{\alpha}F_1 &\geq 0\,,\end{aligned} \tag{17}$$

which form, therefore, necessary conditions for equality in the bounds of Theorem 3.

Proof for the sufficient conditions Now we start with the assumption that the conditions (17) are fulfilled. Let us define the following POVM elements :

$$\begin{aligned}E_0 &= \Sigma^{-1}\sqrt{\rho_0}\left(\rho_0-\alpha F_0\right)\sqrt{\rho_0}\Sigma^{-1}\\ E_1 &= \Sigma^{-1}\sqrt{\rho_1}\left(\rho_1-\frac{1}{\alpha}F_1\right)\sqrt{\rho_1}\Sigma^{-1}\\ E_? &= \Sigma^{-1}\left(\sqrt{\alpha}\sqrt{\rho_0}+\frac{1}{\sqrt{\alpha}}\sqrt{\rho_1}V^\dagger\right)F_0\left(\sqrt{\alpha}\sqrt{\rho_0}+\frac{1}{\sqrt{\alpha}}V\sqrt{\rho_1}\right)\Sigma^{-1}\end{aligned} \tag{18}$$

First, let us verify that this is indeed a valid POVM. The three operators are positive since they are of the form $A\dagger MA$ where M is a positive hermitian operator. In the first two cases this is true because of the conditions (17), in the third case it follows from the positivity of F_0. The three operators sum up to identity, $E_0+E_1+E_?=\mathbb{1}$, as can be checked by straight forward calculation which makes use also of Eqn. (6). Next, we have to check that the given POVM is a valid USD POVM, that is, $\mathrm{Tr}(\rho_0E_1)=\mathrm{Tr}(\rho_1E_0)=0$. This relation holds since the supports of ρ_0 and ρ_1 do not overlap. Therefore, corollary 1 applies and we have $\rho_0\Sigma^{-1}\rho_1=0$ from which follows that $\sqrt{\rho_0}\Sigma^{-1}\rho_1=0$ and $\sqrt{\rho_1}\Sigma^{-1}\rho_0=0$.Finally, one can check in a straight forward calculation exploiting the properties used in the previous checks that this POVM lead to the three desired failure probabilities.

Let us note that we have only used the assumption about the non-overlapping supports to prove the sufficiency of the conditions. Their necessity does not require this assumption. ■

V. DISCUSSION

Theorem 4 characterizes under which circumstances the equality of the bounds in Theorem 3 can be obtained. Whenever two mixed density matrices have no overlapping supports and the corresponding two operators in Theorem 4 are positive semidefinite, we can give explicitly the optimum USD POVM.

The first question is to know whether the set of pairs of generic mixed states (a USD problem which is not reducible to some pure state case), that fulfill the constraints $\rho_0-\sqrt{\frac{\eta_1}{\eta_0}}F_0\geq 0$ and $\rho_1-\sqrt{\frac{\eta_0}{\eta_1}}F_1\geq 0$, is empty or not. Actually this set is non-empty. For instance, consider a problem motivated by a four-state quantum key distribution protocol using coherent states [22]. Here it might be of interest for an eavesdropper to distinguish the density matrices $\rho_0=\frac{1}{2}[|\alpha\rangle\langle\alpha|+|-\alpha\rangle\langle-\alpha|]$ and $\rho_1=\frac{1}{2}[|\imath\alpha\rangle\langle\imath\alpha|+|-\imath\alpha\rangle\langle-\imath\alpha|]$, corresponding to the bit value 0 and 1, respectively. In

fact, this pair of states can be represented as geometrically uniform (GU) states [23] as they are related as $\rho_1 = U\rho_0 U^\dagger$ with $U^2 = \mathbb{1}$. They can be represented as operators over a four-dimensional Hilbert space as

$$\rho_0 = \begin{pmatrix} |c_0|^2 & 0 & c_0 c_2 * & 0 \\ 0 & |c_1|^2 & 0 & c_1 c_3 * \\ c_2 c_0 * & 0 & |c_2|^2 & 0 \\ 0 & c_3 c_1 * & 0 & |c_3|^2 \end{pmatrix} \tag{19}$$

with complex coefficients c_i depending on phase and as given in [22], and

$$U = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} . \tag{20}$$

One can show that for these two states the operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1$ are hermitian and positive semi-definite for some regime of the ratio $\frac{\eta_1}{\eta_0}$ around the value $\frac{\eta_1}{\eta_0} = 1$ included into the second regime (for any c_0, c_1, c_2 and c_3 in $\mathbb{C}$). According to Theorem 4, the optimal failure probability is $Q^{\text{opt}} = 2\sqrt{\eta_0 \eta_1} F$ where the fidelity is given by $F = e^{\frac{-|\alpha|^2}{2}} (|\cos \frac{|\alpha|^2}{2}| + |\sin \frac{|\alpha|^2}{2}|)$. Let us note that, in general, those operators are not positive for the whole second regime $F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F}$. Actually this depends on the parameters c_0, c_1, c_2 and c_3 in $\mathbb{C}$. This implies that, in general, the necessary and sufficient conditions are not fulfilled neither for the first regime nor for the third regime for these two coherent states.

Actually two GU states are not necessarily in the set of states that saturate the bound, not even for equal *a priori* probabilities. For example, one can consider the two GU states ρ_0 and $\rho_1' = W\rho_0 W^\dagger$ where ρ_0 is given as above while

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \tag{21}$$

with $c_0 = \sqrt{0.1}$, $c_1 = \sqrt{0.4}$, $c_2 = \sqrt{0.3}$ and $c_3 = \sqrt{0.2}$ and $\eta_0 = \eta_1$. Those states are indeed GU states since $W^2 = \mathbb{1}$. The supports do not overlap. However, one can show that the operators $\rho_0 - F_0$ and $\rho_1 - F_1$ are not positive semi-definite.

As a result, there exist generic mixed states that satisfy the conditions of Theorem 4 and for which a optimal USD strategy can be given. However, there are generic mixed states that do not satisfy the conditions so that it remains to find the optimal failure probability in those cases.

The second remark is about the link between our result and the pure state case. Actually for two pure states, since $F_0 = F|\Psi_0\rangle\langle\Psi_0|$, $F_1 = F|\Psi_1\rangle\langle\Psi_1|$ and $\text{Tr}(P_0\rho_1) = \text{Tr}(P_1\rho_0) = F^2$, the constraints $\rho_0 - \alpha F_0 \geq 0$, $\rho_1 - \frac{1}{\alpha} F_1 \geq 0$ are always fulfilled and our result reduces to the one of Shimony and Jaeger. We can go beyond this remark and find under which conditions our bounds reduce to the ones in [1]. Since our bounds are tighter, the bounds in [1] are reached if and only if, first, the condition in Theorem 4 are fulfilled and, second, the equalities $\text{Tr}(P_0\rho_1) = \text{Tr}(P_1\rho_0) = F^2$ hold (like in the pure state case). This is made more precise in the following corollary to Theorem 4:

Corollary 2 *Necessary and sufficient conditions to saturate the bounds in [1]*
Consider a USD problem defined by the two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to [12]). Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $Tr(F_0) = Tr(F_1)$. We denote by P_0 and P_1, the projectors onto the support of ρ_0 and ρ_1. The optimal failure probability Q^{opt} for USD then satisfies

$$Q^{\text{opt}} = \eta_1 + \eta_0 F^2 \;\Leftrightarrow\; \begin{matrix} \rho_0 - F F_0 \geq 0 \\ \rho_1 - \frac{1}{F} F_1 = 0 \end{matrix} \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq F \tag{22}$$

$$Q^{\text{opt}} = 2\sqrt{\eta_0 \eta_1} F \;\Leftrightarrow\; \begin{matrix} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0 \end{matrix} \text{ for } F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F} \tag{23}$$

$$Q^{\rm opt} = \eta_0 + \eta_1 F^2 \;\Leftrightarrow\; \begin{array}{l} \rho_0 - \frac{1}{F} F_0 = 0 \\ \rho_1 - F F_1 \geq 0 \end{array} \text{ for } \frac{1}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}}$$

The POVM elements that realize these optimal failure probabilities, if the corresponding conditions are fulfilled, are given by

$$\begin{aligned} E_0 &= \Sigma^{-1} \sqrt{\rho_0} \left(\rho_0 - \alpha F_0\right) \sqrt{\rho_0} \Sigma^{-1} \\ E_1 &= \Sigma^{-1} \sqrt{\rho_1} \left(\rho_1 - \frac{1}{\alpha} F_1\right) \sqrt{\rho_1} \Sigma^{-1} \\ E_? &= \Sigma^{-1} \left(\sqrt{\alpha}\sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} \sqrt{\rho_1} V^\dagger\right) F_0 \left(\sqrt{\alpha}\sqrt{\rho_0} + \frac{1}{\sqrt{\alpha}} V \sqrt{\rho_1}\right) \Sigma^{-1} \end{aligned} \tag{24}$$

with $\alpha = F$ for the first regime, $\alpha = \sqrt{\frac{\eta_1}{\eta_0}}$ for the second regime and $\alpha = \frac{1}{F}$ for the third regime.

In the first regime we find that $E_1 = 0$ because this operator is hermitian, positive semi-definite and its trace vanishes. The resulting POVM has to be a projective measurement with projections onto the support of ρ_1 and onto its orthogonal complement, i.e. $E_0 = P_1^\perp$, $E_1 = 0$ and $E_? = P_1$. A direct proof from the explicit expressions in Eqn. (18) is difficult, however a simple reasoning allows to verify this statement. We consider only the non-trivial case where the supports of ρ_1 and ρ_2 are not identical. Of course, a two-element USD POVM satisfies $E_0 + E_? = \mathbb{1}$ with $\mathcal{S}_{E_0} \subset \mathcal{S}_{\rho_1}$. Then its structure must be such that $E_? = P_1 + R$ where P_1 is the projection onto the support of ρ_1 and R is an operator with support $\mathcal{S}_R \subset \mathcal{S}_{\rho_1}^\perp$ which satisfies $E_0 + R = P_1^\perp$. Then it follows that $Q = \eta_1 + \eta_0 \mathrm{Tr}(P_1\rho_0) + \eta_0 \mathrm{Tr}(R\rho_0)$. In our non-trivial case we will have $\mathrm{Tr}(R\rho_0) > 0$ as soon as $R \neq 0$. Therefore we find as an optimal solution within this class of two-element USD POVM, the POVM with $R = 0$ leading to $E_? = P_1$ and $E_0 = P_1^\perp$. We can actually write the failure probability as $Q^{\rm opt} = \eta_1 + \eta_0 F^2$. Indeed $\rho_1 = \frac{1}{F} F_1$ then $\rho_1^2 = \frac{1}{F^2} \sqrt{\rho_1} \rho_0 \sqrt{\rho_1}$. This implies $F^2 \rho_1 = P_1 \rho_0 P_1$ and finally $\mathrm{Tr}(P_1\rho_0) = F^2$. This is consistent with the results derived above and gives the correct failure probability. In the third regime, we have $E_0 = 0$ and the corresponding POVM is a projective measurement with $E_0 = 0$, $E_1 = P_0^\perp$, $E_? = P_0$.

Finally, let us note that the optimal error probability for the minimum error discrimination strategy is $Q_{\rm MED}^{\rm opt} = \frac{1}{2}\left(1 - \mathrm{Tr}(|\eta_1\rho_1 - \eta_0\rho_0|\right)$ [2]. Then, on one hand the trace distance is related to the minimum error discrimination while on the other hand the Fidelity is related to the unambiguous state discrimination strategy.

VI. CONCLUSION

To summarize, we have given new bounds on the failure probability of unambiguously discriminating two mixed states. Moreover, we provide necessary and sufficient conditions for two mixed states to saturate those bounds. With that result, we give the optimal USD POVM of a wide class of pairs of mixed states. This class corresponds to pairs of mixed states for which the lower bounds (one for each of the three regimes depending on the ratio between the *a priori* probabilities) on the failure probability Q are saturated. This class in non empty since it contains some pairs of generic mixed states as well as any pair of pure states. For those pairs, we provide the first analytical solutions for unambiguous discrimination of generic mixed states. This goes beyond known results which are all reducible to some pure state case. Additionally, we showed that there exists pairs of mixed states that cannot saturate the bounds.

Acknowledgments

We would like to thank Janos Bergou for discussions and drawing our attention to the problem whether the bounds found by Rudolph *et al.* can always be reached. Further, we thank Ulrike Herzog for transmitting a manuscript of [11] prior for publication. Finally we thank Aska Dolinska and the whole QIT group for very useful discussions. This work was supported by the DFG under the Emmy-Noether program, the EU FET network RAMBOQ (IST-2002-6.2.1) and the network of competence QIP of the state of Bavaria (A8).

[1] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301(R) (2003).
[2] C. W. Helstrom, *Quantum detection and estimation theory* (Academic Press, New York, 1976).
[3] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[4] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[5] A. Peres, Phys. Lett. A **128**, 19 (1988).
[6] A. Peres and D. R. Terno, J. Phys. A:Math. Gen. **31**, 7105 (1998).
[7] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).
[8] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
[9] Y. Sun, J. A. Bergou, and M. Hillery, Phys. Rev. A **66**, 032315 (2002).
[10] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. Lett. **90**, 257901 (2003).
[11] U. Herzog and J. Bergou, quant-ph/0502117 (2005).
[12] P. Raynal, N. Lütkenhaus, and S. van Enk, Phys. Rev. A **68**, 022308 (2003).
[13] J. Fiurasek and M. Jezek, Phys. Rev. A **67**, 012321 (2003).
[14] Y. C. Eldar, M. Stojnic, and B. Hassabi, Phys. Rev. A **69**, 062318 (2004).
[15] Y. Feng, R. Duan, and M. Ying, Phys. Rev. A **70**, 012308 (2004).
[16] H. Barnum, C. Caves, C. Fuchs, R. Jozsa, and Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[17] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[18] P. Lancaster and M. Tismenetsky, *The Theory of Matrices, 2nd edition with applications*, Computer Science and Applied Mathematics (Academic Press, Inc., San Diego, 1985).
[19] J. Fill and D. Fishkind, SIAM. J. on Matrix Analysis and Appl. **21(2)**, 629 (1998).
[20] W. J. Anderson and R. Duffin, J. of Math. Analysis and Appl. **26**, 576 (1969).
[21] G. Marsaglia and G. Styan, Canad. Math. Bull. **15(3)**, 451 (1972).
[22] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).
[23] Y. Eldar and G. Forney, IEEE Trans. Inf. Theory **47(3)**, 858 (2001).